PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of:	)	**<u>Group Art Unit</u>: 2137**
	)	
Harald VATER *et al.*	)	**<u>Examiner</u>: Z. Davis**
	)	
Serial Number: 09/700,656	)	***Attorney Docket*: VATE3001/BEU**
	)	
Filed: February 14, 2001	)	**<u>Confirmation No.</u>: 2137**

For: Access-Controlled Data Storage Medium

REQUEST FOR REHEARING (37 C.F.R. §41.52)

Sir:

This is a Request for Rehearing from the Decision on Appeal dated August 16, 2012.

The request is on the basis that the Board has misapprehended or misunderstood the Appellant's argument concerning why the method of Kocher could not have been obviously modified to obtain the claimed method, based on a detailed understanding of what is actually taught by Kocher. In particular, while Kocher teaches some of the steps of the claimed invention, the steps are in an order that makes it impossible to modify the method of Kocher to obtain the claimed invention. The necessary modification involves not just pre-storing of secret keys, as taught by Cordery, but fundamentally altering the method of Kocher in a way that is not even remotely suggested by Cordery.

This is not an argument based on speculation, and is not an argument against physical combination of the references, as implied by explanation on page 4 of the Decision on Appeal, but rather a detailed review of the actual teachings of Kocher, which are relevant to a determination of the "collective teachings" of the references relied on by the Board.[1]

[1] It is noted that these same teachings are relied upon by the Board for its conclusion of obviousness, but that the Examiner and Board consider them in much less detail. Furthermore, it is respectfully noted that these teachings are not found in the earliest priority application for the Kocher publication (**provisional application 60/087,880, dated January 2, 1998**), which is the only priority application having a date prior to the effective filing date of the present application (**May 18, 1998**). Therefore, the Kocher publication is not actually prior art with respect to the present application, and the Appellant intends to re-open prosecution if this Request for Rehearing is unsuccessful.

The relevant teachings of Kocher, described in detail beginning on page 12 of the Appeal Brief, are as follows:

As explained on page 12 of the Appeal Brief, Kocher teaches an array *dataIn,* described in paragraphs [0068] to [0073], which corresponds to the claimed input data. Also as explained on page 12 of the Appeal Brief, Kocher teaches random bits *b*, which correspond to the claimed auxiliary data (Z). The correspondence between the claimed input data/auxiliary function values and Kocher's data array *dataIn* and random bits *b* can be understood from the fact that random bits *b* of Kocher are used to falsify the input data in array *dataIn*, This is specifically explained in paragraph [0072] if Kocher, and is the same blinding operation recited in the initial input data falsifying step of claim 1.

Furthermore, also as pointed out on page 12 of the Appeal Brief, Kocher teaches the following input data-falsifying blinding operation:

dataIn [p] ^ b = dataIn [perm[i]] ^ b,

with "^" indicating a modulo operation. In particular, in the table labeled "Blinded High Entropy Permutation," the sixth to last line of col. 7 (described in the Appeal Brief as the third "for loop") includes the definition of a temporary array as "***dataIn [p] ^ b*** ," with the application of permutation *perm* being indicated in the eighth line from the bottom (**p = perm [i]**).

As further explained on page 12 of the Appeal Brief, Kocher teaches two operations that are performed on the input data. One is a permutation defined by the array "*table*" and another is the permutation defined by the array "*perm*," included in the above blinding operation The operation *perm* changes the order in which the operations involved in applying permutation "*table*" are carried out. Since *table* and *perm* are the only operations carried out on the input data (other than blinding), one or both of these operations must correspond to the claimed operation *f.*

The operation *perm*, which randomizes operation *table*, is explained in greater detail in paragraph [0071] of Kocher:

> Initialization of the blinded randomized-order permutation operation involves constructing and randomizing a permutation table ("perm") for determining the bit order for operations. (Bit order permutation table "perm" randomizes the time at which any particular data bit is manipulated). The bit order table is created in two passes, where the first assures that the table has the correct form (i.e., contains the numbers zero through 63), and the second introduces random order into the table. Because the process of constructing the bit order table does not involve any secret inputs, the only security requirement for the process is that the final result be unknown to attackers.

This passage is summarized on page 12 of the Appeal Brief, by stating that "the additional permutation *perm* is used to avoid processing the steps to compute the permutation *dataOut* in input order or in output order."

Page 12 of the Appeal Brief, overlooked in the Decision on Appeal, thus identifies the data falsification (or blinding step) step performed by Kocher as "***dataIn [p] ^ b***", the primary operation performed on the input data as **[*table*]**, and a randomizing operation [***perm***] carried out to change the order of steps performed by the primary operation *temp.* Consequently, it can be understood that Kocher teaches:

- *falsifying the input data by combination with auxiliary data (Z)*, and
- *execution of the one or more operations (f) on the semiconductor chip.*

Further, it can be understood from paragraph [0074] that Kocher teaches the step of:

- *combining the output data determined by said executing of the one or more operations (f) with said auxiliary function value (f(Z)) in order to compensate for the falsification of the input data.*

However, as further explained on page 12 of the Appeal Brief, what Kocher does not teach is that the step of falsifying the input data is carried out:

- "***<u>before</u>*** *execution of the one or more operations (f),"*

and further that:

- the auxiliary function value used to retrieve the output data is "retrieved from a memory of said semiconductor chip of the data carrier" and "*previously determin*[*ed*]. . .*by execution*

of the one or more operations (f) with the auxiliary data (Z) as input data in safe surroundings."

In other words, it can be understood from the teachings of Kocher that Kocher teaches a method involving blinding of input data and recovering the data using auxiliary function values, but not blinding of input data *before* execution of one or more operations *f*, and not pre-storage of auxiliary function values. **In order to obtain the claimed invention, therefore, the method of Kocher must be modified by:**

(a) **performing the step of falsifying the input data *before* execution of the operations *f (i.e., temp* and/or *perm*), and**

(b) **using pre-stored auxiliary function values to recover the original input data, as allegedly suggested by Cordery's teaching that secret keys may be protected by storing them on a secure data carrier.**

<u>This was the position of the Examiner adopted by the Board</u>. The problem with this conclusion is that such a modification of Kocher's secure data processing method is **<u>NOT POSSIBLE</u>** without modifying the method of Kocher in a way that is not suggested by Kocher and certainly not suggested by Cordery.

The problem with applying the teachings of Cordery to the method of Kocher in the manner suggested by the Examiner and adopted by the Board is that, as explained on page 12 of the Appeal Brief, **<u>the blinding operation depends on the permutation operation</u>**, which can only be carried out **AFTER** at least one of the operation steps is performed. This can be understood by the step of applying the modulo operation to the permutation operations as well as the input data:

dataIn [p] ^ b = dataIn [perm[i]] ^ b.

This operation is necessary to generate the auxiliary function values used to recover the original input data and undo the blinding operation. Furthermore, the appropriate unblinding vector is stored in the array *dataOut* and already **computed together with the blinded input vector, *i.e.*, in the same for-loop defined by *dataOut table[p] := b.*** Thus, it can be understood from Kocher that **<u>the data-recovery blinding operation cannot be carried out until the permutation is carried out,</u>**

***i.e.*, until at least one operation is performed on the input data.**[2] Moreover, since blinding occurs after application of the permutation operation *perm*, which randomizes the operations *temp*, then it follows that the auxiliary function values compensate for the effect of the blinding operation on output data represented by *dataOut* **cannot be predetermined and pre-stored**.

Paragraphs [0072] and [0071] of Kocher explain in detail the reasons for constructing *perm* before blinding. As explained, for example, in paragraph [0071], lines 9-15, of the Kocher publication:

> ***Because the process of constructing the bit order table does not involve any secret inputs, the only security requirement for the process is that the final result be unknown to attackers**. As illustrated, the first permutation table initialization loop can also place random values into dataOut and tempt to help whiten any leaked signals when data values are first stored in these arrays (emphasis added).*

---

[2] By way of background, though not necessary to understand the argument presented in this Request for Rehearing, the exact method of blinding used by Kocher is given in the form of source code included in paragraph [0068], as follows (THIS FOOTNOTE IS COPIED FROM THE FIRST APPEAL BRIEF, FILED ON DECEMBER 20, 2006):

- Suppose the length of the input array dataIn is 64. An array *perm* holding the numbers from 0 to 63 in a randomly permuted manner is computed in a first step (see the first and second for-loops of the listed source code).
- In a second step, another array *temp* of length 64 is computed by setting for every I from 0 to 63:
  temp [p] := dataIn [p] ^ b,
  where ^ denotes the XOR operator, b is a random bit just computed, and p = perm [I], *i.e*, p is an index given by the previously computed random array perm.
- In a third step (also in the second for-loop), dataOut is temporarily set to dataOut [table [p]] = b (see the third for-loop of the listed source code).
- In a fourth step, the array perm is recomputed, *i.e.*, randomly permuted once more (see the fourth for-loop), although the general algorithm would work without this step.
- Finally, in the last step, the input data dataIn is finally permuted by setting, for every I from 0 to 63, where again p = perm[i]:
  dataOut [table [p]] := temp [p], which is the same as
  dataOut [table [p]) := dataIn[p] ^ b (see the second step above).

The blinding of the input data by the random bit b is compensated for by setting:
dataOut [table [p]] ^:= temp [p], which is a shorthand notation for
dataOut [table[p]] := dataOut [table[p]] ^ temp [p].

Summarizing, one obtains from the temp [p] correlations and the expression dataOut [table [p]] = b obtained in the third step described above:
dataOut [table[p]] := b ^ dataIn[p] ^ b = dataIn[p], which is what was originally to be computed since b ^ b = 0.

It can be seen from this analysis of the blinding method listed in paragraph [0068] of Kocher that only the order in which the operations dataOut [table [p]] := dataIn [p] were performed is permuted by the random permutation *perm*, by setting p = perm [I] where I runs from 0 to 63. Furthermore, the input bits dataIn [p], where temporarily blinded by the random bits b are compensated for after the permutation of the blinded input bits.

In particular, the first step of the claimed method, namely <u>falsifying of input data</u> (dataIN), is carried out by combination with auxiliary data in the form of random bits b before the execution of one or more operations (the permutation of the array dataIN according to the order given by the source code). The second step of the claimed method, namely <u>compensation for the falsification</u>, is carried out by determining the output data by the execution of one or more operations (dataIn [p] ^ b = temp [p]) combined using dataOut [table [b] ^= temp [p] with an auxiliary function value (dataOut [table [b]] = b). However, the third step, namely <u>computing the auxiliary data (random bits b) and auxiliary function value (the permutation of b temporarily stored as dataOut [table [p]])</u>, *is carried out* <u>while</u> *computing the permutation of the input data***.**

Furthermore, the last two sentences of paragraph [0072] of Kocher explain that:

> *Additionally, the output buffer (dataout) is the result of using the input permutation table to operate on the index to temp. The second part of the blinding process re-randomizes the bit order permutation table (perm).*

In other words, as described in the above-cited passages and argued in the Appeal Brief, Kocher teaches an approach that integrates data input blinding with operation randomization (represented by *perm*). In order to modify the method taught by Kocher to obtain the claimed invention, **it would be necessary to disregard Kocher's teachings concerning application of the randomizing permutation *perm* before all of the data is blinded** Nothing in Kocher suggests doing so, nor is it possible to pre-determine and therefore pre-store the "auxiliary values" required to recover the input data after permutation and blinding. If anything, the highlighted passage in paragraph [0072] teaches that pre-storing of auxiliary data is unnecessary, and suggests that this would be undesirable because it would add security requirements that are rendered unnecessary by the use of *perm* (the "bit order table").

These teachings in Kocher of carrying out operation permutations in conjunction with data blinding are clearly incompatible with the claimed blinding-before-operations and pre-calculation and storage of the auxiliary function data. In order to obtain the claimed invention based on the "collective teachings" of Kocher and Cordery, it would have been necessary to ignore the specific teachings of Kocher that blinding and permutation operations are carried out at the same time in the same loop so that "***the only security requirement for the process is that the final result be unknown to attackers**.*" Cordery provides absolutely no motivation for ignoring the teachings of the Kocher in this manner, since Cordery does not concern random values used in data blinding, or randomization of operations, but merely teaches protection of secret keys. Kocher method has nothing to do with protection of secret keys, which would still need to be kept safe even if used as part of the operations *temp* that are randomized by *perm*, while Cordery is concerned with protection of data that clearly must be predetermined, *i.e.*, keys, and not with temporary values used during a randomization operation.

In summary, Kocher does not teach the claimed method, except for pre-storage of certain data, as argued by the Examiner. Kocher instead teaches some of the steps of the claimed method, but rearranged and including a randomization operation that make it impossible to pre-store auxiliary function values as claimed. Since Cordery merely teaches that secret keys may be pre-stored, and does not in any way suggest eliminating randomization operations in order to modify the method of Kocher in such a way as to enable pre-storage of auxiliary function values, the proposed combination of Kocher and Cordery would not have resulted in the claimed invention.

It is respectfully noted that these arguments are based solely on the teachings of Kocher and are not at all speculative in nature, but rather simply require a detailed reading and understanding of the specification of Kocher. The fact that they are attorney arguments should not be dispositive. The attorney is merely pointing out what is taught by the references, which is surely permitted. Since the aforementioned teachings of Kocher are incompatible with the claimed invention, are part of the "collective teachings" of Kocher and Cordery, and are uncontradicted by any other teachings in Kocher or Cordery, it cannot reasonably be said that the "collective teachings" of Kocher and Cordery suggest the claimed invention.

Conclusion

For all of the foregoing reasons, rehearing of the Decision on Appeal and reversal of the Examiner's final rejection of claims 26-33 and 42 under 35 U.S.C. §103(a) is improper and should be reversed by this Honorable Board.

Respectfully submitted,

BACON & THOMAS, PLLC

/Benjamin E. Urcia/

Date: October 16, 2012 By: BENJAMIN E. URCIA
Registration No. 33,805

BACON & THOMAS
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314
Telephone: (703) 683-0500

S:\Producer\beu\Pending Q...Z\V\VATER 700656\RequestForRehearing.wpd